UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

MALINDA A. SMIDGA, KAYLA MANDENG, and FRANCES CURD, *individually and on behalf of all others similarly situated*, Plaintiffs, v. SPIRIT AIRLINES, INC., Defendant.	Case No. 2:22-cv-01578-MJH

EXHIBIT B

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

INDIA PRICE, ERICA MIKULSKY, MARILYN HERNANDEZ, DANIEL RUBRIDGE, and ARIEL OLIVER, individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

CARNIVAL CORPORATION,

Defendant.

Case No.: 23-cv-236-GPC-MSB

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS

[ECF No. 23]

Pending before the Court is Defendant Carnival's Motion to Dismiss Plaintiffs' First Amended Complaint. A hearing was held on January 12, 2024. For the reasons stated below, the motion is **GRANTED IN PART AND DENIED IN PART.**

BACKGROUND

Carnival, "the world's largest leisure travel company," maintains a website at carnival.com where users may browse and book cruises. On carnival.com, no action goes unnoticed. Every click is counted, every keystroke is collected, and every cursor movement is catalogued. Carnival explains that this constant surveillance "improve[s]"

the user experience, ECF No. 23 ("Motion to Dismiss" or "MTD") at 12,[1] but Plaintiffs prefer to browse in privacy, and bring suit alleging that Carnival has violated federal wiretap and hacking laws and seven state analogues.

Plaintiffs allege that Carnival enlists third-party companies to embed recording software, often referred to as "Session Replay Code," on Carnival's website. ECF No. 22 ("First Amended Complaint" or "FAC") at ¶¶ 1, 67. One such party is Microsoft. *Id.* at ¶ 51. Microsoft calls its Session Replay Code, "Clarity," and embeds Clarity on Carnival's "website, either by directly hard-coding the code on the website or through a third-party platform . . . ." *Id.* at ¶ 59. When a user visits the website, Clarity is "deploy[ed]" onto the user's browser. *Id.* at ¶ 50. There, it collects information about the user's system, including their device, browser, operating system, and location, as well as "all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry (even if deleted), and numerous other forms of a user's navigation and interaction through the website." *Id.* at ¶¶ 31, 53. Clarity transmits the collected information to Microsoft's server in "hyper-frequent logs" which are "often just milliseconds apart." *Id.* at ¶¶ 31, 72.

After recording the user's information, Microsoft "analyze[s]" it. *Id.* at ¶ 2 ("Both Carnival and the Session Replay Providers access and analyze the video replay of the user's behavior on the website."). Microsoft provides Carnival with a reenactment of the user's visit, akin to "a video replay," *id.* at ¶ 2, and uses Clarity to create "detailed heatmaps" for Carnival, "that provide information about which elements of a website have high user engagement," *id.* at ¶ 55. Clarity's most powerful function, however, is its ability to expose a user's browsing on other sites. *See id.* at ¶ 42. Clarity attaches a "specific user ID," or a "fingerprint," to a visitor's profile based upon their unique

---

[1] Page citations refer to CM/ECF pagination.

"combination of computer and browser settings, screen configuration, and other detectable information." *Id.* at ¶¶ 41, 53. Carnival accesses these fingerprints, which are collected across every site that Clarity is deployed on, and uses them to link a user's session to "web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous." *Id.* at ¶¶ 41–42, 190, 220. Plaintiffs allege that Carnival uses Microsoft's services to create "unique IDS and profiles" for each of its users, *id.* at ¶ 70, "de-anonymizing" its users' internet browsing, *id.* at ¶¶ 190, 220.[2]

Plaintiffs complain that as a result of this practice, Carnival intercepts Plaintiffs' personal information,[3] including their "passport number, driver's license number, date of birth, home address, phone number, email address and/or payment information," *id.* at 11, and uses that information to trace users' browsing history on other sites in violation of the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*, the Computer Fraud and Abuse Act, 18 U.S.C. §1030, the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq.*, the Maryland Wiretapping and Electronic Surveillance Act, Md. Code Ann., Cts. & Jud. Proc. § 10-401, *et seq.*, the Massachusetts Wiretap Act, Mass. Gen. Laws ch. 272, §99, the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons.

---

[2] Plaintiffs allege that Carnival makes similar use of "other Session Replay Code through various Session Replay Providers," including a company known as ContentSquare. *Id.* at ¶¶ 63–64.

[3] Because Plaintiffs have made more than general allegations that their personal data was intercepted, the Court concludes that Plaintiffs "have made sufficient allegations to create a question of fact as to whether there is sufficiently personal information to support [Article III] standing." *See James v. Walt Disney Co.*, No. 23CV02500EMCEMC, 2023 WL 7392285, at *6 (N.D. Cal. Nov. 8, 2023); *see also Steel Co. v. Citizens for Better Env't*, 523 U.S. 83, 94 (1998) (holding that standing is a "question the court is bound to ask and answer for itself, even when not otherwise suggested").

Stat. § 5701 *et seq.*, and each of the aforementioned states' common-law prohibitions on invasion of privacy.

LEGAL STANDARD

On a motion to dismiss under Rule 12(b)(6), the Court takes as true all well-pleaded factual allegations set forth in the complaint and construes them in the light most favorable to the Plaintiffs. *Benavidez v. Cnty. of San Diego*, 993 F.3d 1134, 1158 (9th Cir. 2021). To survive a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

ANALYSIS

1. Wiretap Claims

i) Party to the Communication Exception

To plead a plausible claim under the Federal Wiretap Act, Plaintiffs' complaint must demonstrate that Carnival (1) without consent (2) intentionally intercepted the (3) contents of a communication (4) using a device. *See* 18 U.S.C. §2511. Carnival submits that, as an initial matter, its surveillance scheme escapes the purview of federal and state wiretap laws because Plaintiffs intended to communicate with Carnival.[4] *See* 18 U.S.C. §

[4] The federal and state wiretap laws are treated as largely analogous. MTD at 16; *see, e.g.*, *Pena v. GameStop, Inc.*, 2023 WL 3170047, at *3 (S.D. Cal. 2023) ("'The analysis for a violation of CIPA [Cal. Penal Code § 631] is the same as that under the federal Wiretap Act.'"); *Com. v. Blystone*, 519 Pa. 450, 464-65 (1988) ("[T]he Pennsylvania wiretapping statute is based on its federal counterpart, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2016."); *Davis v. State*, 43 A.3d 1044, 1051 (Md. 2012) ("[I]t is clear through both legislative history and case precedent that the federal wiretap statute … served as the guiding light for the Maryland Act; therefore, we read the acts in pari materia."); *Com. v. Vitello*, 367 Mass. 224, 251 (1975) ("[I]n substance the requirements of the Massachusetts statute are the same as

2511(2)(d) ("It shall not be unlawful . . . for a person . . . to intercept a[n] electronic communication where such person is a party to the communication.").[5] Wiretapping requires a third party to the communication. *See Tanner v. Acushnet Co.*, 2023 WL 8152104, at *4 (C.D. Cal. Nov. 20, 2023). "That alone," Carnival insists, ends Plaintiffs' wiretap claims. ECF No. 26 ("Carnival Reply") at 12.

But Carnival's surveillance scheme employs third parties, like Microsoft. *See* MTD at 28 ("Carnival . . . procured third-party Session Replay Providers . . . ."). While some courts have construed software providers as "extensions" of the websites that employ them where the software "merely function[s] as a tape recorder," courts decline to adopt this construction where the software performs more than the ordinary function of a tape recorder. *Acushnet*, 2023 WL 8152104, at *4 (quoting *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 898 (N.D. Cal. 2023)). Software providers exceed the "ordinary function of a tape recorder" where, for instance, they "capture[], store[], and interpret[] real-time data." *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021). Here, Plaintiffs allege that Clarity processes Plaintiffs' data to generate analytics, including heatmaps of user engagement and unique IDS and profiles containing their browsing history on other websites. FAC at ¶¶ 42, 55 ("Clarity also uses the information captured to create detailed heatmaps of a website . . . ."). Plaintiffs allege that Carnival makes active use of those capabilities. *See, e.g.*, *id.* at ¶ 101 ("Carnival's subsequent use of data, in a manner for which it lacked permission, namely associating the data with user's pre-existing online activity and using it to advertise . . . violated . . .

---

those of Title III [the Federal Wiretap Act], as the legislative history of Title III shows that they should be.").

[5] Plaintiffs conceded at oral argument that the "party to the communication" exception would apply if Carnival recorded user communications without the assistance of a third party.

the Wiretap Act."). Because generating heatmaps and fingerprinting unique browser profiles extends beyond the function of a tape recorder, the "party to the communication" exception does not prevent Carnival from being "held liable under [] federal and state wiretapping statutes for directing, aiding and/or abetting its Session Replay Provider[, Microsoft,] to integrate Session Replay Code into its website." ECF No. 25 ("Plaintiffs' Opposition") at 14.[6]

ii) Consent

Carnival next argues that Plaintiffs consented to recording by (1) the "very act of sending a communication over the internet and by (2) constructively assenting to the terms of Carnival's Privacy Policy. The Court considers these arguments in turn.

Citing *Commonwealth v. Proetto*, A.2d 823, 829 (Pa. Super. 2001), Carnival argues that Plaintiffs' "very act of sending a communication over the Internet" to Carnival constituted express consent to Carnival's surveillance scheme—its simultaneous transmission of Plaintiffs' communications to a third party for collection and processing, tagging of Plaintiffs' browser profiles, and tracing of their visits on carnival.com to visits on other websites.[7] *See* MTD at 18. *Proetto* stands for the common-sense premise that an individual that sends a message over the internet, like an individual leaving a message on an answering machine, is "aware of the fact that messages are received in a recorded format . . . and can be downloaded or printed by *the party receiving the message*" and "if

---

[6] As discussed below, the Court dismisses one of Plaintiffs' claims with leave to amend. That leave extends to the entire complaint, and Plaintiffs may plead facts further describing how Clarity processes the collected data.

[7] Plaintiffs argue that Carnival may not raise the issue of consent at the motion to dismiss stage, *see* Plaintiffs' Opposition at 8 n.4, but "[c]onsideration of consent is appropriate on a motion to dismiss where [as here] lack of consent is an element of the claim." *Silver v. Stripe Inc.*, 2021 WL 3191752, at *2 (N.D. Cal. 2021).

not deleted by *the receiver*, will remain on *the receiver's* system." *Id.* at 830 (emphasis added). Relying upon the answering machine analogy, the *Proetto* court concluded that defendant had expressly consented to the fifteen-year-old complainant's decision, to save the email and chat-room messages that defendant had sent to her, and report them to the police department. *Id.*

Proetto did not discuss simultaneous interception by a third party, because the communication at issue occurred without a third-party eavesdropper. The complainant "received the communication[s] and *later* disclosed th[ose] communication[s] to Detective Morris." *Id.* at 829 (emphasis added). Moreover, peppered through *Proetto's* analysis of consent is the court's emphasis that consent is given—not to anyone who happens upon the communication—but to "the receiver." *Id.* at 829–30. Nowhere does *Proetto* discuss consent to a third party. That absence is critical, here, where Carnival must demonstrate that Plaintiffs' consent extends not just to the receiver, Carnival, but also to third-party Session Replay Providers, like Microsoft.

In an attempt to bridge this gap, Carnival cites to *Farst v. AutoZone, Inc.*, 2023 WL 7179807, at *4 (M.D. Pa. 2023). There, the court dismissed plaintiff's Session Replay Code claims in the context of online shopping, reasoning that shopping is a public activity and that use of the internet to shop does not change that. *Id.* (citing *Cook v. GameStop, Inc.*, 2023 WL 5529772, at *4 (W.D. Pa. Aug. 28, 2023) and *Massie v. Gen. Motors LLC*, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022)). But *Farst*, and the cases it cites, center their reasoning on the plaintiffs' failure to plead that defendants had intercepted personal information or something beyond mere "shopping preferences." *See Farst*, 2023 WL 7179807, at *5 ("Farst does not aver AutoZone disclosed his home address, credit card, bank account, social security number, or any other information that could potentially be used to identify him"); *Cook*, 2023 WL 5529772, at *4 ("Ms. Cook did not enter any personally identifying information at any point during her interaction.

Not her name. Not her address. Not her credit card information. Nothing that could connect her browsing activity to her."); *Massie*, 2022 WL 534468 at *5 ("Each of Plaintiffs' cited cases involves the collection and disclosure of personal information. Here, Plaintiffs do not allege that any of their information collected by the Session Replay software was personal or private . . . ."). *Farst* distinguished its holding, from cases recognizing an internet privacy interest, based upon "[t]he type of data collected in those cases," which included "plaintiffs' genders, birthdates, IP addresses, browser settings, and unique device identifiers." 2023 WL 7179807, at *4. This is the exact information that Plaintiffs allege Carnival captured. *See, e.g.*, FAC at ¶ 35. Indeed, the court in *Farst* granted plaintiff leave to amend, noting that "[m]any of the deficiencies identified herein with respect to the concreteness of Farst's asserted injury are factual and thus potentially curable." 2023 WL 7179807, at *6. Plaintiffs' pleading here possesses what Farst's pleading lacked: concrete assertions that Carnival intercepted personal information. Accordingly, Carnival's citation to *Farst* only weakens its position. The Court concludes that Plaintiffs' internet communications to Carnival did not constitute consent to recording by third parties, especially where Plaintiffs have adequately plead the interception of sensitive, personal information including their passport numbers and credit cards. *See In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 600–03 (9th Cir. 2020).

Carnival's second argument is that it provided Plaintiffs notice of Carnival's recording policy via a "Cookie Policy" banner displayed at the bottom of Carnival's website, and that Plaintiffs constructively assented to the terms of that policy through their continued use of the site. But Plaintiffs allege that the website does not put Plaintiffs on notice of recording, and that "users can interact with Carnival's website without ever reviewing or agreeing to the terms of any purported privacy policy Carnival

may have." FAC at ¶ 70. At this stage, where the Court must take as true the Plaintiffs' well-pleaded factual allegations, Carnival's consent defense appears premature.

Carnival disputes this, noting that the Court need not accept as true "any allegations that are contradicted by matters . . . incorporated by reference in a complaint." MTD at 14–15. Carnival observes that the website is incorporated into Plaintiffs' complaint by reference, and invites the Court to consider several screenshots. MTD at 13 n.1; see also Knievel v. ESPN, 393 F.3d 1068, 1076 (9th Cir. 2005) (holding that internet pages are incorporated by reference where "plaintiff's claim depends on the contents of a document").[8] Carnival argues that the screenshots demonstrate that the Cookie Policy banner "immediately overlays the bottom of the visitor's browser window" and "persists at the bottom of the carnival.com website as a visitor navigates the site, even if they click through different pages." MTD at 14–15.[9] But a screenshot without additional information cannot demonstrate that a banner appears "immediately" or that it "persists" throughout a user's visit. Screenshots capture only a moment in time and cannot reflect Carnival's temporal assertions.

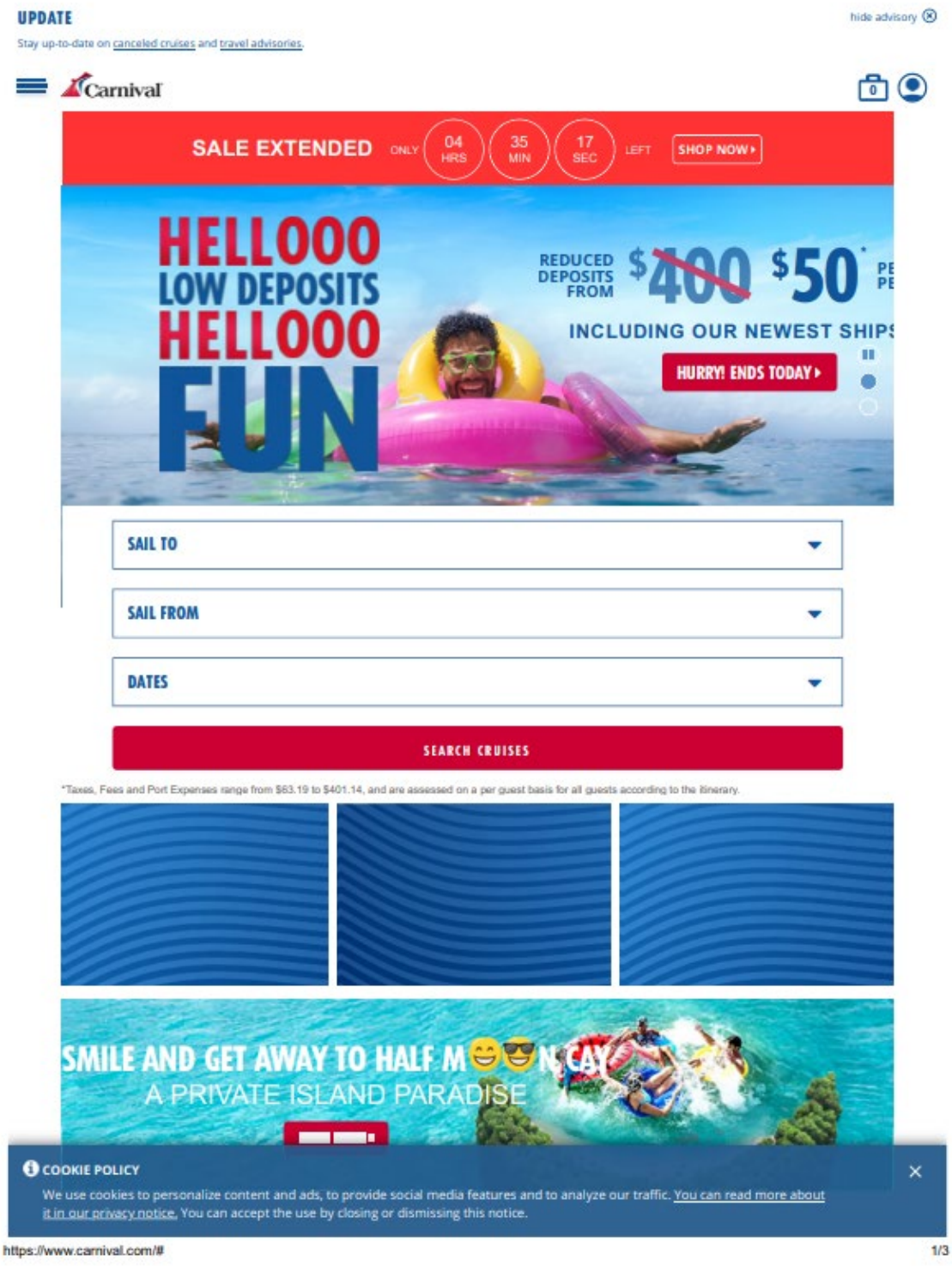
Furthermore, Carnival's screenshots, which Carnival acknowledges may not be accurate representations of what Plaintiffs viewed, MTD at 14 n.2, do not demonstrate that Plaintiffs were on notice of Carnival's recording policy. Carnival attempts to provide notice of its recording policy with a banner located at the bottom of a user's screen, otherwise known as browsewrap, "a notice that—by merely using the services of, obtaining information from, or initiating applications within the website—the user is

---

[8] Plaintiffs do not object, and the Court incorporates the screenshots by reference.

[9] Carnival insisted at oral argument that the Court may not independently visit Carnival's website to verify these assertions.

agreeing to and is bound by the site's terms of service." *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176 (9th Cir. 2014). Pictured below, is one of Carnival's screenshots.



ECF No. 18-2 at 2. The "Cookie Policy" banner informs users that Carnival "use[s] cookies to personalize content and ads, to provide social media features and to analyze [Carnival's] traffic." *Id.* The banner includes a hyperlink, that users may click to view Carnival's privacy policy. *Id.*

"[W]here, as here, there is no evidence that the website user had actual knowledge of the agreement, the validity of the browsewrap agreement turns on whether the website puts a reasonably prudent user on inquiry notice of the terms of the contract." *Nguyen*, 763 F.3d at 1177 (citing *Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17, 30–31 (2d Cir. 2002). "Whether a user has inquiry notice of a browsewrap agreement, in turn, depends on the design and content of the website and the agreement's webpage. *Id.* (citing *Be In, Inc. v. Google Inc.*, 2013 WL 5568706, at *6 (N.D. Cal. Oct. 9, 2013)). Courts have declined to enforce browsewrap agreements where notice is hidden at the bottom of a page, *see In re Zappos.com, Inc. Customer Data Sec. Breach Litig.*, 893 F. Supp. 2d 1058, 1064 (D. Nev. 2012), appears in small print, *see Pollstar v. Gigmania, Ltd.*, 170 F. Supp. 2d 974, 981 (E.D. Cal. 2000), or is only visible to users if they have scrolled down to the next screen, *Specht*, 306 F.3d at 23.

Here, the Cookie Policy banner, is visible to a user without scrolling. However, the text of the banner is smaller than the rest of the bold, large typeface found on Carnival's homepage, the notice is placed far below the relevant buttons that a user may click, the blue of the banner matches the blue of other web panels, and the white text of the banner blends in with the website's white background. Additionally, Carnival has not demonstrated that the banner appears immediately or that the banner persists for the entirety of a user's visits. Taken together, these facts do not demonstrate that a "reasonably prudent user [would be] on inquiry notice of the terms of [Carnival's Privacy Policy]." *Ngyuen*, 763 F.3d at 1177. A user may be distracted by the large red buttons inviting them to "SHOP NOW" or "SEARCH CRUISES" and never view the slim

banner across the bottom of their screen. A user may click one of these large, red buttons before the Cookie Policy banner appears, and the banner may fail to appear on subsequent pages. Whether because of the notice's small text, inconspicuous color scheme, or potential failure to appear, a reasonably prudent user would not "necessarily have known or learned of the existence of [Carnival's privacy] agreement prior to acting . . ." *See Specht*, 305 F.3d at 30. Accordingly, the Court credits Plaintiffs' allegations and concludes that at this stage, Plaintiffs have sufficiently alleged that interception of their communications occurred without their consent.[10]

iii) Interception

To demonstrate interception, Plaintiffs must allege that their communications were "acquired during transmission, not while [they were] in electronic storage." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002). In other words, the collection without consent of Plaintiffs' information must occur contemporaneously with its ordinary transmission. Plaintiffs allege:

> 68. During visits by Plaintiffs to www.carnival.com and its subpages, Plaintiffs browsed for cruise packages and different destinations. Plaintiffs communicated with Carnival's website by using their mouse to hover and click on certain links and items, and inputting personal information and information about potential trips they were researching or planning. All of this information – both record data and the content of each Plaintiff's Website Communications -- was intercepted by the Session Replay Code and sent to the Session Replay Provider during those visits.
>
> 69. The Session Replay Code immediately and instantaneously captured Plaintiffs' Website Communications for the entire duration of their visits. Indeed, through

---

[10] In their amended complaint, Plaintiffs may choose to further detail Plaintiffs' experiences with Carnival's cookie policy banner. Plaintiffs may take this opportunity to supplement their description of the cookie banner, including as to whether the banner consistently loads, whether the banner follows the user as they navigate the website, and whether the banner appears for subsequent users of a shared computer.

> Carnival's deployment of Session Replay Code, Plaintiffs' Website Communications were automatically and secretly intercepted while using Carnival's website.

See FAC at ¶ 68.

Plaintiffs also allege that Session Replay Code, implanted in their browser, captured their actions at hyper-frequent intervals, often just milliseconds apart, and then communicated those actions at hyper-frequent intervals to Session Replay Provider servers. *See id.* at ¶¶ 31, 72. Thus, Plaintiffs submit, they have alleged sufficient facts to demonstrate that "transmission of a website user's Website Communications . . . happens contemporaneously in real-time." FAC at ¶ 31.

At oral argument, Carnival emphasized that the internet is not magic and relied heavily upon its contention that content is "packetized" and electronically stored, but much of the technical detail counsel relied upon is not found in the pleadings. [11] Drawing all reasonable inferences in favor of Plaintiffs, the Court finds that Plaintiffs have plausibly alleged that interception occurs contemporaneously with transmission. At this stage, the Court finds that it may reasonably infer that at least some transmission and interception occurred contemporaneously, within the same span of milliseconds. *See James v. Walt Disney Co.*, No. 2023 WL 7392285, at *14–15 (N.D. Cal. Nov. 8, 2023); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 841 (N.D. Cal. 2014).

iv) Contents

[11] During oral arguments, both sides discussed transmission in terms of "packets." That term is not found in the pleadings. Thus, Plaintiffs may find it prudent in their amended complaint to further detail how Plaintiffs' actions are transmitted to Carnival's website and detail the timelines of transmission and interception.

The wiretapping laws at issue apply only where a defendant "acqui[res] . . . the contents of any wire, electronic or oral communication." 18 U.S.C. 2510(4).[12] "Contents" means "information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). Carnival emphasizes that "content" does not include "record information," such as the "'name,' 'address,' and 'subscriber number or identity' of a subscriber or customer," when such information is merely "generated in the course of the communication." *In re Zynga Privacy Litig.*, 750 F.3d at 1107; MTD at 24. But record information may constitute "contents" where "the record is the subject of a communication . . . ." *Id.*

The Ninth Circuit approved the First Circuit's decision in *In re Pharmatrak*, 329 F.3d 9, 15, 18–19 (1st Cir. 2003), where the First Circuit held that defendant had "intercepted the content of the sign-up information customers provided to pharmaceutical websites, which included their 'names, addresses, telephone numbers, [and] email addresses . . .' and provided this information to third parties." *See id.* ("[T]he First Circuit correctly concluded that the defendant was disclosing the contents of a communication."). The Ninth Circuit reasoned that "[b]ecause the users had communicated with the website by entering their personal medical information into a form provided by the website, the First Circuit correctly concluded that the defendant was disclosing the contents of a communication." *Id.* Here, Plaintiffs have alleged that "[t]he data and information intercepted by the Session Replay Code . . . includ[es], *inter alia*, Plaintiffs' location, intent to travel, dates of travel, travel locations as well as other

---

[12] MTD at 14 n.7; 18 Pa. Stat. § 5702 (requiring the "acquisition of the contents of any wire, electronic or oral communication"); Md. Code Ann., Cts. & Jud. Proc. § 10-401(10) (same); Mass. Gen. Laws Ann. ch. 272, § 99(B)(4) (requiring the acquisition of "the contents of any wire or oral communication"); Cal. Penal Code § 631 (making it unlawful to "read[], or attempt[] to read, or to learn the contents or meaning of any message, report, or communication").

personal data requested to book travel plans such as passport number, driver's license number, date of birth, home address, phone number, email address and/or payment information." FAC at ¶ 35.[13] Just as in *Pharmatrak*, this information was "entered into an information field or text box" provided by Carnival's website. FAC at ¶ 1. The Court finds that Plaintiffs have alleged the capture of personally identifiable information that is the subject of the communication, and thus Plaintiffs have sufficiently alleged the interception of "contents."

v) Device

The wiretapping laws at issue apply where interception is accomplished "through the use of any electronic, mechanical, or other device." 18 U.S.C. 2510(4).[14] Plaintiffs allege that "Plaintiffs' and Class members' browsers and computing device and Defendant's webservers, website, and the Session Replay Code Defendant deployed are all 'devices' for the purposes of the Wiretap Act." FAC at ¶ 92. Carnival contends that Plaintiffs' wiretapping claims are all premised on Carnival's use of "Session Replay Code", computer code, which does not constitute a "device" within the meaning of the wiretap laws. MTD at 18. According to Carnvial, if "device" is interpreted to require a

---

[13] At oral argument, Carnival suggested that credit card information is not "contents" because such information may be obtained by a federal prosecutor under 18 U.S.C. § 2703. But Carnival is not a "governmental entity" and has not been issued a "warrant" by a "court of competent jurisdiction." *See id.* Thus, even to the extent that 18 U.S.C. § 2703 would have any application to the instant case, the Court finds Carnival's argument unpersuasive.

[14] This is true of the Federal law, along with Pennsylvania's, Maryland's, and Massachusetts's. *See* MTD at 26; 18 Pa. Stat. § 5702 (requiring the "acquisition of [a] communication through the use of any electronic, mechanical or other ***device***" (emphasis added)); Md. Code Ann., Cts. & Jud. Proc. § 10-401(3) (same); Mass. Gen. Laws Ann. ch. 272, § 99(B)(4) (requiring acquisition "through the use of any intercepting ***device***" (emphasis added)). California's wiretapping law does not include the device limitation, and so is not affected by this section of the order.

physical object, "Carnival's use of computer code [would] not constitute a 'device' within the meaning of the wiretap laws . . . ." MTD at 29. However, this perspective is overly circumscribed because it views the computer code in a vacuum, separate and apart from the computer that executes it. *See James v. Walt Disney Co.*, No. 2023 WL 7392285, at *13 (N.D. Cal. Nov. 8, 2023) ("It is artificial to claim that software must be viewed in isolation from the computing device on which it runs and with which it is inseparable in regard to the challenged conduct."). After all, software is no more than "a set of instructions, known as code, that directs a *computer* to perform specified functions or operations." *Fantasy Sports Prop v. Sportsline.com*, 287 F.3d 1108, 1118 (Fed. Cir. 2002) (emphasis added); *see also Google LLC v. Oracle Am., Inc.*, 141 S. Ct. 1183, 1191-92 (2021) ("But how do you as the programmer tell the computer which of the implementing code programs it should choose, i.e., which task it should carry out?"). All software, regardless of the language it is written in or the complexity of its function, requires hardware to execute it. *See TiVo, Inc. v. EchoStar Commc'ns Corp.*, 516 F.3d 1290, 1309 (Fed. Cir. 2008) ("As an initial matter, software alone cannot extract data from a physical device; it can only control hardware that extracts data."). As Carnival reminded this Court at oral argument, the internet is not magic. Like a recipe without a chef, or sheet music without a musician, software cannot function—much less collect and transmit data at hyper-frequent intervals to a third party—without hardware to run it. Because a computer that executes software is undoubtedly a physical device, the motion to dismiss fails on these grounds as well.[15]

In conclusion, the Court **DENIES** Carnival's Motion to Dismiss as it relates to the wiretap claims.

---

[15] Plaintiffs may choose to supplement existing allegations with additional facts describing the use of a server or webserver to execute Session Replay Code.

2. Invasion of Privacy Claims

To state an invasion of privacy claim, Plaintiffs must allege "conduct by the defendant that amounts to a serious invasion of [a] protected privacy interest." MTD at 31 (quoting *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 829 (N.D. Cal. 2020)).[16] The invasion must be "'highly offensive' or 'serious.'" *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 830. "Courts have repeatedly found the surreptitious recording of a plaintiffs' conversations or activity to constitute an actionable intrusion." *Id.* Furthermore, under California law, determining whether an intrusion is highly offensive often "cannot be conducted at the motion to dismiss stage where, as here, there are open factual questions regarding 'the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive.'" *Id.* (quoting *In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 606 (9th Cir. 2020)); *see also Tanner v. Acushnet Co.*, 2023 WL 8152104, at *7 (C.D. Cal. Nov. 20, 2023) ("[C]ourts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is."); *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (same); *D'Angelo v. Penny OpCo, LLC*, 2023 WL 7006793, at *11 (S.D. Cal. Oct. 24, 2023) (same). However, the same is not true under Pennsylvania law. *See Boring v. Google Inc.*, 362 F. App'x 273, 279 (3d Cir. 2010).

---

[16] The four states' treatment of privacy claims is largely the same. *See* MTD at 31 n.11; *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 122 (W.D. Pa. 2019); *Branyan v. Sw. Airlines Co.*, 105 F. Supp. 3d 120, 126 (D. Mass. 2015) ("[T]o prevail on a claim alleging an invasion of privacy, a plaintiff must prove that there was … an unreasonable, substantial or serious interference with his privacy."); *see also Demo v. Kirksey*, 2018 WL 5994995, at *3 (D. Md. 2018) ("Maryland and Pennsylvania have adopted the same definition for intrusion upon seclusion.").

Thus, the Court undertakes the analysis and concludes that Plaintiffs have alleged facts sufficient to establish a serious invasion of a protected privacy interest.

Carnival's position relies on *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 830, for the proposition that data collection is "nothing more than . . . 'routine commercial behavior," and that a defendant engaging in such behavior "does not commit an invasion of privacy." MTD at 32. But the court in *In re Google Assistant Privacy Litig.*, specifically rejected this argument, finding "[n]onetheless," that "a reasonable person could find Defendants' alleged conduct to be 'highly offensive.'" *Id.* Carnival further submits that its actions cannot be "highly offensive" because "even collection of 'plaintiff's HIV status'" does not constitute "highly offensive" behavior. MTD at 31 (quoting *McNemar v. The Disney Store, Inc.*, 91 F.3d 610, 622 (3d. Cir. 1996)). This is, of course, a gross oversimplification of *McNemar*. *McNemar* held that plaintiff did not state a claim for invasion of privacy where his store manager, in an attempt to be supportive, asked him whether he was HIV-positive. 91 F.3d at 622. The court noted that this was hardly coercive, "let alone 'highly offensive to a reasonable person.'" *Id.* The court further held that a store manager's disclosure of plaintiff's HIV-positive status to plaintiff's friend, who already knew he was HIV-positive, was "not sufficient to state a *prima facie* case of invasion of privacy for publicity given to private facts." *Id.* Neither of these holdings bear any relevance to the present case.

Courts addressing cookie-enabled surveillance schemes dismiss invasion of privacy claims where plaintiffs allege nothing more than the collection of "keystrokes, mouse clicks, and [personally identifiable information]." *See Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 122 (W.D. Pa. 2019); *see also Williams v. DDR Media, LLC*, 2023 WL 5352896, at *6 (N.D. Cal. Aug. 18, 2023); *Farst*, 2023 WL 7179807, at *4. But courts decline to dismiss invasion of privacy claims where plaintiffs allege that the intercepted information is used to compile a user's browsing history across other

websites. *See Revitch*, 2019 WL 5485330, at *3 (finding that intrusion "which allegedly allowed NaviStone to associate Revitch's browsing habits with his identity, is a highly offensive breach of norms"); *Griffith v. TikTok, Inc.*, 2023 WL 7107262, at *6 (C.D. Cal. Oct. 6, 2023) (holding that because "the Tiktok [software development kit] allows Defendants to assemble extensive profiles containing individuals' browsing histories across numerous websites . . . the Court cannot conclude at the pleading stage that the alleged privacy intrusion is not serious"); *cf. Williams*, 2023 WL 5352896 at *6 (contrasting plaintiffs' allegations with allegations in *Facebook Internet Tracking*, 956 F.3d at 596, where "plaintiffs alleged Facebook captured . . . plaintiffs' internet activity and turned it into detailed 'personal profiles'"); *Farst*, 2023 WL 7179807, at *4 (contrasting plaintiff's allegations with cases where defendants "compiled users' internet-wide search histories, create[ing] detailed user profiles"). This case falls into the latter category, as Plaintiffs have alleged that Carnival used the intercepted information to "back-reference all of [a] user's web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous." FAC at ¶ 42. Accordingly, the Court finds that Plaintiffs have sufficiently pleaded their invasion of privacy claims.

3. Computer Fraud and Abuse Act ("CFAA")

To state a claim under the CFAA, Plaintiffs must plead facts showing that Carnival "intentionally acesse[d] a computer without authorization or exceed[ed its] authorized access, and thereby obtain[ed] … information from [the] protected computer." 18 U.S.C. § 1030(a)(2)(C). Plaintiffs must also demonstrate that they suffered "damage or loss" under one of the factors set forth in § 1030(c)(4)(A)(i)(I)–(V). Plaintiffs attempt to invoke two of these factors, FAC at ¶¶ 107–08, contending that Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least

$5,000 in value," and constituted "a threat to public health or safety," *see* 18 U.S.C. § 1030(c)(4)(A)(i)(I), (IV).

But Plaintiffs' allegations of damage or loss are entirely conclusory. The complaint "merely parrots the language of the statute without providing any factual allegations." *James v. Veros Credit, LLC*, 2019 WL 13102877, at *2 (S.D. Cal. 2019). To the extent Plaintiffs suggest that Carnival's interception "deprive[d Plaintiffs] of the economic value of their own information," Plaintiffs' Opposition at 22, Plaintiffs fail to "plausibly allege that they intended to sell their non-disclosed personal information to someone else. Nor, in any event, do they plausibly allege that someone else would have bought it as a stand-alone product." *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 784 (N.D. Cal. 2019). And to the extent Plaintiffs suggest that Carnival's actions pose a threat to public health or safety because of "identity theft and online scams," they have failed to allege facts demonstrating the threat is anything more than speculation. *See id.*; *see also Dahlia v. Rodriguez*, 735 F.3d 1060, 1076 (9th Cir. 2013) (holding that court may "reject, as implausible, allegations that are too speculative to warrant further factual development.").

The Court dismisses Plaintiffs' CFAA claim with leave to amend, to the extent that Plaintiffs may do so in good faith.

CONCLUSION

The Court **GRANTS IN PART AND DENIES IN PART** Carnival's Motion to Dismiss. Plaintiffs' CFAA claim is dismissed with leave to amend. The Court declines to dismiss Plaintiffs' wiretap and invasion of privacy claims.

IT IS SO ORDERED.

Dated: January 19, 2024

Hon. Gonzalo P. Curiel
United States District Judge